services provided by the LEC-owned and non LEC-owned LIDBs are identical, there is no justification for the existing disparate treatment. More importantly, to the extent the FCC intends the LIDB tariff obligations to be an effective fraud minimization tool, the FCC must ensure that the obligations extend to all LIDB providers.

- The LIDB tariffs of all LIDB providers should contain information informing LIDB users of the potential for fraud notwithstanding the use of the LIDB.

- The LEC data owners should clarify their procedures for responding to customer fraud referrals, and commit to certain operational standards for informing their LIDB provider of such referrals.

- LIDB providers must better coordinate communications between their fraud detection centers and the LEC data owner's inquiry office to reduce customer confusion.

- The FCC should adopt rules holding all carriers and LIDB providers harmless from end user complaint where the carrier has refused to carry ABS calls, or where the LIDB provider has deactivated a calling card or imposed billed number screening on a line number, due to legitimate fraud concerns.

- The FCC should recognize that liability cannot be assigned solely through provisions in the LIDB provider's

(Footnote Continued)
with which data updates are made from the time of receipt, and the type of information stored in the database.

tariffs. Rather, each industry member should bear responsibility for toll fraud losses in proportion to its ability to control the incidence of fraud.

V. CONCLUSION.

Sprint firmly supports efforts to improve coordination among customers, service and equipment providers, and regulatory and law enforcement agencies to combat toll fraud. To that end, Sprint has worked closely with such entities; has implemented an active anti-fraud customer education program; and believes that 18 U.S.C. Section 1029 should be amended to specifically reference telecommunications toll fraud. Sprint also endorses the general principle that assessment of toll fraud liability should reflect each party's ability to prevent and detect fraud, and has integrated such principle in its business operations. Adoption of this general principle, rather than specific rules or formulas which attempt to assess liability, should be sufficient to protect the interests of affected parties. Should this general principle prove to be unworkable or insufficient, the Commission could revisit the issue at a future date.

There are a number of measures which can be taken to reduce the risk of payphone and cellular toll fraud, including subscription to OLS and BNS services; installation of equipment or software which identifies a line as a payphone; use of the 8000 and 9000 numbering scheme for payphones; transmission of relevant information digits in the call detail record which identifies cellular calls; implementation of pre-call verification procedures for all cellular calls; and adoption of a Part 22 rule which requires cellular phone design which prohibits transmission of anything other than the original factory-installed ESN.

Similarly, there are several measures which can be taken to minimize ABS-related fraud, including commitment to specific LIDB operational standards governing (among other things) fraud trigger thresholds, handling of customer fraud referrals, and normal and emergency updates by LIDB providers; provision and use of "called from/called to" numbers; and improved coordination between LEC data owners and LIDB providers.

Respectfully submitted,

SPRINT CORPORATION

Norina T. Moy

Jay C. Keithley
Michael B. Fingerhut
Norina T. Moy
1850 M St., N.W., Suite 1110
Washington, D.C. 20036
(202) 857-1030

Craig T. Smith
P.O. Box 11315
Kansas City, MO. 64112
(913) 624-3065

January 14, 1994

ATTACHMENT A

Con artists today are continually looking for new ways to rip-off consumers. That's why you have to be aware of some of their tricks. We designed this brochure to help you avoid some of the methods they use.

A valid calling card number is like gold to con artists. They can take that number and sell it to others, open international calling lines, put it on a computer network, etc. One key rule to follow is to immediately notify your long distance company whenever you think someone has acquired your card number.

You might not be able to stop all scam artists, but if you use these common-sense tips, you'll make it a lot more difficult for them to operate.

Produced jointly by:

NACAA

National Association of Consumer
Agency Administrators
1010 Vermont Ave., N.W., Suite 514
Washington, D.C. 20005
(202) 347-7395

Sprint

Toll Fraud Prevention
1510 E. Rochelle
Irving, Texas 75039

Printed on recycled paper.
Please recycle and encourage others to do so.

PHONE

A Southern California resident received a call from a friendly representative of a long distance company who wanted to verify the customer's calling card number because, the representative said, "It looks like someone might be using it for fraudulent purposes."

The elderly man wanted to be helpful and gave the number to the caller. Imagine the man's shock when his monthly bill was nearly $30,000, with calls to countries around the world.

☎ ☎ ☎

A gentleman thought his phone bill seemed thicker than normal. It was a huge surprise when it contained 35 pages of long distance charges to places around the globe. His normal monthly bill was about $30 each month. This one was for $1,180!

☎ ☎ ☎

These are just a few sad results from industry-wide long distance scams that are being pulled on innocent people each and every day. In one year alone, toll fraud scams like these will exceed $1 billion in the long distance industry. And, while you do not have to pay directly for unauthorized charges if you report them to your long distance carrier promptly, you eventually pay for this theft through higher prices.

The good news is that you can reduce the potential for toll fraud by taking just a few simple precautions. This brochure will highlight some of the more common forms of fraud and what you can do to avoid them.

Your phone rings at home, and a nice-sounding man says he is with the phone company. He says there have been numerous calls made on your calling card number, and he wants to verify your card number with you. . .

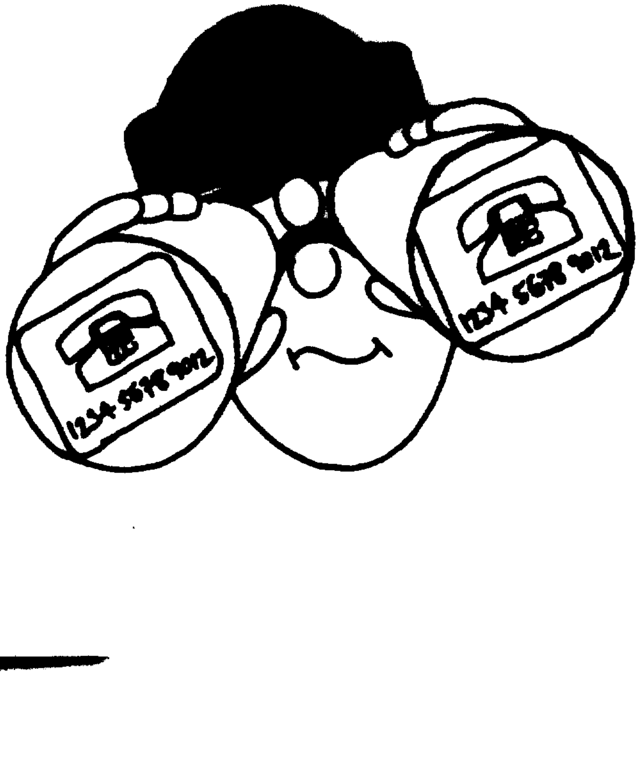
Action To Take

Never give your telephone card number over the phone to anyone calling you, whether they say they are with a phone company (or, for that matter, a federal agency, police department, etc.) Phone companies do not call customers to verify numbers – they already know them! However, if you do give your number out – for whatever reason – notify your phone company right away. The card number can be cancelled and a new number issued almost immediately.

You go to a pay phone to make a long distance call. You read the number of your calling card to the operator while holding up your long distance card to read it. . .

Action To Take

Be extremely careful with your calling card number, particularly in public places, such as airports. Con artists use binoculars and cameras – and even pretend to be using an adjoining phone – in order to steal numbers from unsuspecting victims. Cover up your card so others cannot see it. If you must read it aloud, make sure others cannot overhear it. If the phone has a digital display of your number, cover it. If you even suspect someone has stolen it, immediately notify your phone company.



You are moving to a new home. With all the activity you forget to notify your long distance carrier of your move. . .

Action To Take

A phone bill sent to a vacant home is an open invitation to crooks to steal the phone card number. Always notify your local and long distance telephone companies when you are planning a move so that your final bill will be sent to your new address and service will be re-established correctly at your new destination.

Your phone rings and an operator says she has Fred on the line and he would like to charge a long distance call to your number. Your husband's name is Fred. . .

Action To Take

Are you sure it's your husband calling? Why not ask the operator to let you verify the person's voice? Frequently, con artists look in a phone book and ask an operator to call a number and simply use the husband's (or wife's) first name for verification. If the voice on the other end is familiar, go ahead and let them bill a call to your phone if you want. If not, tell the operator "no."

Always verify any person (company or agency) before allowing any calls to be charged to your phone.

To stop potential calling card fraud remember these tips:

☎ Do not give your calling card number to anyone who is calling you.

☎ Protect your number when placing calls in public places.

☎ Prior to moving, notify your long distance carrier where to forward your bill.

☎ Don't allow anyone to charge calls to your phone without verification.

☎ Call your long distance company immediately if you feel your calling card number has been compromised in any way.

☎ Consumers are not required to pay for unauthorized charges on their phone bill. Follow the procedure outlined on your bill for notifying your long distance company about any disputed charge.

Sprint.

SPRINTGUARD℠

SprintGUARD℠ and SprintGUARD Plus℠ AVAILABILITY AND PRICING

SprintGUARD, Sprint's comprehensive security support service, reduces your risk of financial jeopardy by protecting your voice and data network systems from unauthorized intrusions.

SprintGUARD includes a comprehensive set of security services, including technical assistance, traffic monitoring and analysis, training courses and ongoing support. Together, these services have proved effective in minimizing Sprint customers' vulnerability to computer hacking and other unauthorized systems usage – and the financial loss that accompanies it.

SprintGUARD

SprintGUARD is available to all Sprint business customers at no extra charge.

SprintGUARD Plus

SprintGUARD Plus is available to all Sprint business customers. SprintGUARD Plus customers must have a service term plan with Sprint .

CUSTOMER FINANCIAL EXPOSURE	$10,000 PER CPE FRAUD INCIDENT
MONTHLY CHARGE PER CPE CONFIGURATION	$100 ($5,000 MAXIMUM)
ONE-TIME ACTIVATION FEE PER CPE CONFIGURATION	$100 ($5,000 MAXIMUM)

Contractual terms and conditions will apply.

The Facts About SprintGUARD Plus^{SM}

SPRINTGUARD^{SM}

Can your business afford a major financial loss caused by hacking and CPE fraud? Get guaranteed financial protection with SprintGUARD Plus.

SprintGUARD Plus significantly limits your financial loss while providing specialized security services to defend against unauthorized telecommunications usage.

Fraud is a business that is growing at an alarming rate, costing U.S. companies as much as $2 billion each year – and every telecommunications user is a potential victim. It's likely that you can't risk the potential financial losses caused by unauthorized system access – Private Branch Exchange (PBX), Centrex, voice mail and auto attendant fraud. SprintGUARD Plus provides the extra protection that minimizes your exposure to abuse while limiting your losses when fraud does occur.

Financial protection against CPE fraud

Unexpected losses hit you directly on the bottom line. Through SprintGUARD Plus, Sprint will take financial responsibility for any CPE fraud incident incurring more than $10,000 at a customer premises equipment (CPE)* location – the lowest cap in the industry. Not surprisingly, Sprint was the first telecommunications company to offer this type of financial protection to customers.

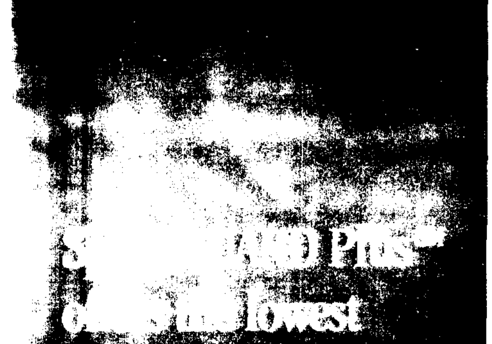
Coverage for key Sprint services

International and 800 calling is increasingly important to businesses. SprintGUARD Plus covers all Sprint inbound domestic 800 and inbound international toll-free calls and all international outbound calls that originate from your CPE. This includes calls to every country as well as calls to area code 809.

Comprehensive daily fraud analysis

For SprintGUARD Plus customers, every inbound domestic 800 and inbound international toll-free call is also monitored and analyzed, 365 days a year. Sprint notifies customers of suspected abnormal calling patterns.

Sprint.



SprintGUARD Plus℠ offers the lowest cap in the industry for shared financial responsibility for CPE fraud.

Timely fraud reports to eliminate "surprises"

Immediately upon detection, Sprint can automatically fax to you complete call detail reports for the suspected fraud. Complete historical call detail for all calls occurring since your previous invoice is available within five business days of the detection – so there are no unexpected costs when you receive your next month's invoice.

A dedicated CPE Security Support Manager

One of our experienced CPE Security Support Managers will be assigned to work with you throughout a CPE fraud incident to provide assistance and recommend corrective action. You'll also receive investigation support and assistance in working with legal authorities in cases of prosecution.

Ongoing bulletin updates

You'll receive periodic bulletins for keeping abreast of the most current information and practices about CPE fraud and prevention methods.

The value-added benefits of SprintGUARD Plus CPE Security Support go straight to your bottom line – and beyond.

- Financial protection against CPE fraud. Decreasing the cost associated with unauthorized users of your CPE facilities helps increase your company's profit margin.

- Prompt, personalized attention. Sprint's CPE Security Support Managers, professionals with wide-ranging technical and consultative expertise, can help you with any and all of your CPE security concerns.

- Proven effectiveness. Sprint's customers' average loss per CPE fraud occurrence ($1,350) on the Sprint network is the lowest in the industry.

- Additional protection through SprintGUARD℠. SprintGUARD Plus customers also receive all the benefits of SprintGUARD CPE Security Support Services.

To assist us in providing these services, Sprint asks your cooperation in performing these required activities to maximize your protection.

- Use a minimum of eight digits for each Direct Inward System Access (DISA) code. Sprint Corporate Security will suggest an alternative security method if a CPE doesn't support eight digits.
- Eliminate voice mail, auto attendant and all other external call transfer capabilities, including the ability to transfer or route traffic to the trunk level.
- Install a security system on all CPE remote maintenance ports.
- Delete all default passwords.
- Complete a Customer Profile form for each CPE.
- Provide Sprint Corporate Security with telephone numbers of three individuals who can be notified at any time if Sprint detects fraud originating from a CPE.
- Advise Sprint's Corporate Security Department of changes in emergency contacts or CPE Customer Profile information.
- Develop an action plan to be implemented in the event of a CPE fraud detection.

As the first company to provide a network security service that limits its customers' financial loss, Sprint will continue enhancing protective measures to provide the highest level of service reliability. Please call your Sprint Representative today for details.

RESTRICTIONS: SprintGUARD Plus does not cover fraud on another carrier's network, calls on the Sprint network other than the types mentioned in this product brief, or fraudulent calls terminating within the United States (other than inbound domestic 800 and inbound international toll-free calls). The service does not cover fraud resulting from customer negligence, employee disclosure of proprietary information, improper installation of CPE software or equipment or improper execution of procedures. Sprint will not be liable for charges occurring after four hours and within 14 days after we notify the customer of suspected CPE fraud. Contractual terms and conditions will apply. This service is not available for resellers of Sprint network services in support of their customers.

* Customer financial losses of $10,000 are per incident, per CPE and are based on pre-discounted toll-free inbound or outbound usage. Sprint's portion of the CPE fraud will be credited net of discounts to the customer's account. Sprint's maximum CPE fraud credit will not exceed $1 million per CPE per incident.

SPRINTGUARD SM

- **CPE security education service.** Sprint will provide educational programs on such important topics as how to protect your CPE from fraud, partnering solutions for avoiding fraud and the background of CPE abuse as an industry-wide problem.

- **Fraud prevention assistance**. Sprint will consult with you to help identify your system's vulnerabilities and recommend the most effective defense measures against potential costly abuse.

- **Investigation support.** Sprint's Corporate Security staff – located in Atlanta, Chicago, Dallas, Denver, Kansas City, New York, Sacramento, San Francisco and Washington, D.C. – are available to evaluate system security, recommend corrective action and assist you in working with legal authorities.

- **Emergency call tracing.** Centralized emergency call-tracing support is provided 24 hours a day, 365 days a year.

- **Domestic and international carrier liaison assistance**. Sprint will interface with other domestic and international carriers to assist you in resolving your security threats.

- **Law enforcement and prosecution support** Sprint will provide professional security support and serve as the interface between you and the appropriate law enforcement agency.

SprintGUARD's proactive approach makes a world of difference in reducing your security risk.

- **Minimal exposure.** Sprint features the lowest national average of CPE fraud per incident – $1,350 on the Sprint network compared to the national average of $60,000 per incident.

- **Optimal network availability**. Because SprintGUARD deters hackers and other network abusers from causing traffic congestion, Sprint customers can feel confident that lines will be available whenever they're needed.

- **Proven effectiveness.** SprintGUARD CPE Security Services have been key in minimizing fraudulent CPE traffic for Sprint's customers. In fact, international CPE fraud on Sprint's network was less than 1 percent of the 1992 industry estimate for total international CPE fraud losses.

As the first company to offer its customers a combined voice and data network security service, Sprint will continue to enhance protective measures to provide you with the highest levels of service possible. Call your Sprint Representative today for details.

* Not available to resellers of Sprint network services in support of their customers.

Sprint assumes no liability for CPE fraud.

Sprint.

The Facts About SprintGUARD℠ CPE Security Support Serv

SPRINTGUARD℠

SprintGUARD CPE Security Support Services are a highly effective defense against the growing threat of customer premises equipment fraud – and they're yours at no charge.

SprintGUARD is the industry's first combined voice and data network security service for the detection and prevention of unauthorized system access.

Customer premises equipment (CPE) fraud costs U.S. businesses from $1 billion to $2 billion annually. Whether it's a thrill-seeking computer hacker who disrupts CPE systems or an outsider using and reselling your services for personal gain, losses are measured in dollars, time and the unavailability of network services when you need them.

SprintGUARD CPE Security Support Services, value-added services provided at no additional cost to all Sprint business customers,* proactively combat this alarming problem.

Backed by the expertise of the Sprint Corporate Security staff, SprintGUARD keeps watch over your domestic and international Sprint services. We also keep you informed of suspected CPE abuse, so your financial losses are minimized.

- ▶ **Traffic analysis.** Sprint performs selective analyses of outbound international calls – to every country (including area code 809), for every business customer. The same analysis is provided for inbound domestic 800 and inbound international toll-free services.
- ▶ **Electronic bulletin board monitoring.** Sprint monitors domestic and international electronic bulletin boards to identify the misuse of your company's CPE and access codes.
- ▶ **Notification.** Sprint will notify you of abnormal activity that is identified and will recommend corrective action.
- ▶ **24-hour security support.** Telecommunications security support is available to you 24 hours a day, 365 days a year, by calling the Corporate Security Department toll-free at 1-800-877-7330.

Sprint.

ATTACHMENT B

Business Telephone System Security

Telecommunications Fraud

In the U.S. today, toll fraud from business telephone systems (eg. PBX, Voice Mail, etc.) could reach $1 billion this year. While calling-card fraud previously was the number one telecommunications fraud problem, today business telephone fraud has taken over the top spot.

This guide has been developed by United Telephone not only to help you understand the severity of the problem, but also to help you take the necessary steps to minimize the chances of becoming a victim of this crime. A few simple preventative steps might help eliminate thousands of dollars of unauthorized calls – calls you are responsible for paying.

A Growing Problem

Telephone fraud is one of the fastest growing criminal businesses today. A few years ago only a few individuals were capable of tapping into a PBX or Voice Mail system. Today, hackers can access these systems, put "live" numbers on nationwide bulletin boards, or even sell them on the street. Within hours, thousands of unauthorized calls can be placed.

Unfortunately, with the technology available today, no matter what steps you take to guard your telecommunications system, ***there is no 100 percent guarantee that fraud will be prevented.*** Many individuals who are committing this crime today are professionals who stay abreast of current technology and use this knowledge to continuously look for new ways to steal telecommunications services.

One relatively simple step you can undertake to deter toll fraud is to not *allow calls to originate or terminate from specific, nationwide or international area codes that employees wouldn't normally call for business purposes.* Your telecommunications representative may also be able to point out potential high-fraud area codes.

Four Common Methods of Toll Fraud

There are four basic ways computer "hackers" try to access a typical business telephone system and begin amassing toll charges:

1. Remote Access
2. PBX operator assistance
3. Voice Mail
4. Call Diverters

Remote Access Fraud

The Remote Access feature of a business telephone system is one of the inviting tools hackers use to commit toll fraud. This feature is designed to enable long distance calls to be re-originated through a business telephone system from an off-premise location.

Most telephone system remote access features require a Personal Identification Number (PIN) to be dialed by the caller. Unfortunately, most PBX, voice mail and Centrex (ABC) systems are often programmed to accept simple PIN sequences (1234, 1991, 4321, etc.).

To compromise your PIN, the intruder calls your business telephone system via your "800" or other access number, and then dials various combinations until the Remote Access feature PIN is discovered (this often can be done within an hour). Once a valid PIN is found, an unlimited number of calls can be placed – and an unlimited amount of long distance charges can be incurred.

Steps You Can Take

There are a number of things you can do to reduce the chances of having intruders access your remote access feature:

❑ Have the feature disconnected entirely from your telephone system.

❑ Be certain only those individuals with a definite need for remote access are given PINs, and use the maximum number of digits your system will allow. When employees terminate employment, their PIN should be deleted.

❑ Develop random PIN numbering. Avoid patterns, vanity numbers and the manufacturers' default codes, which can be easily discovered. Routinely change all PINs.

❑ Consider a ring delay option. This will cause the telephone system to wait for ring tones before a connection is made. This could fool many hacker dialing programs.

PBX Operator Scheme

In the PBX operator direct dial scheme, the hacker uses conversational skills to persuade a PBX operator to assist in placing a long distance call. The intruder uses your "800" number to call an employee, and then asks to be transferred back to the operator.

Once transferred, the operator assumes the call is originating internally. The intruder often then asks the operator to provide assistance in completing a call. Once an outside line is provided, toll fraud begins.

Steps You Can Take

To reduce or eliminate this problem you can:

❑ Have supervisors routinely verify outbound long distance calls made by their employees.

❑ Make employees aware of this scheme – particularly PBX operators. If dialing assistance is requested, have the operator disconnect and dial back the requesting extension.

Voice Mail Access Fraud

A voice mail system enables the unattended deposit and retrieval of voice messages. Via trial and error, hackers can get into an employee's mailbox, change a valid PIN and take over the mailbox. The stolen PINs can be passed on to other criminals and a voice mail system can be completely overrun by unauthorized users.

Steps You Can Take

To reduce the chance of voice message fraud occurring, you can:

❑ Develop random PIN numbering schemes and avoid using telephone extension numbers as PINs.

❑ Do not publish the telephone number of the voice mail system.

❑ Delete PINs when employees terminate; change PINs regularly.

❑ Review an "Invalid Attempt Report" daily as a potential early warning sign. Have users report any unauthorized messages left in their mailboxes.

The Call Diverter Method

Another method criminals use to place long distance calls is via a Call Diverter. This is a device used to forward calls to a remote location, usually after normal business hours, so that important calls are not missed.

The intruder can scan the Yellow Pages or a Chamber of Commerce Directory to look for professional listings (doctors, lawyers, dentists, etc.) or any business with a need to receive after-hour calls. By determining the type of Call Diverter in use and the answering point, the intruder often calls and claims to have mis-dialed or remains silent and waits for the called party to hang-up. In that brief instant, the intruder will then seize the dial tone and dial long-distance numbers.

Steps You Can Take

Avoiding a Call Diverter scam can frequently be done by:

□ Troubleshooting the Call Diverter system to ensure that dial tone is immediately disconnected when the calling party hangs up.

□ Making employees aware of the risk with Call Diverters. Have your answering service be alert for frequent wrong numbers or silence on the line which could lead them to believe the caller has disconnected.

In Summary

No method of preventing business telephone system toll fraud is perfect. Criminals stopped by one method frequently discover another one. But, by following the steps outlined in this brochure, you will make it much more difficult for fraud to occur.

United Telephone companies are ready to work with you to try and make your system as "hacker-proof" as possible. Call on us.

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing COMMENTS OF SPRINT CORPORATION was sent by United States first-class mail, postage prepaid, on this the 14th day of January, 1994, to the below-listed parties:

Kathleen B. Levitz
Acting Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W., Room 500
Washington, D.C. 20554

Linda Dubroff
Common Carrier Bureau
Federal Communications Commission
2025 M Street, N.W., Room 6008
Washington, D.C. 20554

International Transcription Service
1919 M Street, N.W., Room 246
Washington, D.C. 20554

Christine Jackson

Christine Jackson

January 14, 1994